

Tomohiko Kitamu  
NAK1 - BP67  
(JWP)(949)261-81

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

997 U.S. PTO  
09/921235

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office

出 願 年 月 日  
Date of Application:

2001年 1月26日

出 願 番 号  
Application Number:

特願2001-019267

出 願 人  
Applicant(s):

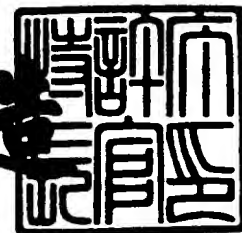
松下電器産業株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 6月25日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



【書類名】 特許願

【整理番号】 2022520271

【提出日】 平成13年 1月26日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 13/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 北村 朋彦

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100090446

【弁理士】

【氏名又は名称】 中島 司朗

【先の出願に基づく優先権主張】

【出願番号】 特願2000-237017

【出願日】 平成12年 8月 4日

【手数料の表示】

【予納台帳番号】 014823

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9003742

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 システム集積回路

【特許請求の範囲】

【請求項 1】 秘密データを格納したメモリデバイスと共に、機器に組み込まれるシステム集積回路であって、

中央処理装置と、

複数の記憶領域を有する記憶手段と、

機器に対する起動操作が操作者によりなされれば、メモリデバイスから秘密データを読み出して、記憶手段における複数領域のうち予め定められた記憶領域に当該秘密データをセットし、その後中央処理装置に対して動作開始を指示する初期化手段と

を備えることを特徴とするシステム集積回路。

【請求項 2】 前記機器は、操作者により起動操作がなされた際、外部リセット信号を出力する外部リセット信号出力手段と、

複数のクロックパルスからなるクロック信号を出力するクロック発振手段とを備え、

前記初期化手段は、

外部リセット信号が出力されれば、クロックパルスの波数を計数するカウンタと、

波数の計数値が第 1 の所定値になれば、メモリデバイスから秘密データを読み出して記憶手段における複数領域のうち、予め定められた記憶領域にセットする読出部と、

波数の計数値が、第 1 の所定値より大きい第 2 の所定値になれば、中央処理装置に対して内部リセット信号を出力して動作開始を指示する出力部と

を備えることを特徴とする請求項 1 記載のシステム集積回路。

【請求項 3】 前記秘密データは、機器についての識別情報又は機器を操作する操作者についての識別情報を暗号化して得た暗号化データであり、

システム集積回路は、

読出部により読み出された暗号化データを復号して、元の識別情報を得る復号

化部を備え、

記憶手段における複数の記憶領域のうち、予め定められた記憶領域は、

復号により得られた元の識別情報を格納する

ことを特徴とする請求項 1 記載のシステム集積回路。

【請求項 4】 前記機器においてメモリデバイスは、バスを介してシステム集積回路と接続されており、

前記初期化手段は、機器に対する起動操作が操作者によりなされれば、秘密データをバスに出力するようメモリデバイスに指示し、その後、バスに出力された秘密データを取り込むアクセス制御部を備える

ことを特徴とする請求項 1 記載のシステム集積回路。

【請求項 5】 前記アクセス制御部は、

命令又はデータを読み出す旨が中央処理装置により指示されれば、命令又はデータをバスに出力するようメモリデバイスを制御し、その後、バスに出力された命令又はデータを取り込み、

データを書き込む旨が中央処理装置により指示されれば、データをバスに出力し、その後、バスに出力されたデータを取り込むようメモリデバイスを制御する

ことを特徴とする請求項 4 記載のシステム集積回路。

【請求項 6】 機器においてメモリデバイスは、シリアル線を介してシステム集積回路と接続されており、

前記初期化手段は、機器に対する起動操作が操作者によりなされれば、秘密データをシリアル線に出力するようメモリデバイスに指示し、その後、シリアル線に出力された秘密データを取り込むアクセス制御部を備える

ことを特徴とする請求項 1 記載のシステム集積回路。

【請求項 7】 前記アクセス制御部は、

命令又はデータを読み出す旨が中央処理装置により指示されれば、命令又はデータをシリアル線に出力するようメモリデバイスを制御し、その後、シリアル線に出力された命令又はデータを取り込み、

データを書き込む旨が中央処理装置により指示されれば、データをシリアル線に出力し、その後、シリアル線に出力されたデータを取り込むようメモリデバイ

スを制御する

ことを特徴とする請求項 6 記載のシステム集積回路。

【請求項 8】 システム集積回路はメモリデバイスと共に、機器に組み込まれ、

機器においてメモリデバイスは、バス及びシリアル線を介してシステム集積回路と、接続されており、

前記初期化手段は、機器に対する起動操作が操作者によりなされれば、秘密データをシリアル線に出力するようメモリデバイスに指示し、その後、シリアル線に出力された秘密データを取り込み、

命令又はデータを読み出す旨が中央処理装置により指示されれば、命令又はデータをバスに出力するようメモリデバイスを制御し、その後、バスに出力された命令又はデータを取り込み、

データを書き込む旨が中央処理装置により指示されれば、データをバスに出力し、その後、バスに出力されたデータを取り込むようメモリデバイスを制御する  
アクセス制御部

を備えることを特徴とする請求項 1 記載のシステム集積回路。

【請求項 9】 前記秘密データは、メモリデバイス固有のデバイス鍵であり

前記初期化手段は、

機器に対する起動操作が操作者により指示されれば、メモリデバイスからデバイス鍵を読み出して、予め定められた記憶領域に格納し、

前記システム集積回路は、

中央処理装置によりデータ書き込みが命じられれば、書き込むべきデータを、記憶領域に格納されたデバイス鍵を用いて暗号化する暗号化手段と、

暗号化されたデータをメモリデバイスに格納させるよう、メモリデバイスを制御するアクセス制御手段と

を備えることを特徴とする請求項 1 記載のシステム集積回路。

【請求項 10】 前記アクセス制御手段は、

中央処理装置によりデータ読み出しが命じられれば、暗号化されたデータを読

み込むようメモリデバイスを制御し、

前記システム集積回路は、

読み込まれた暗号化データを復号して、元のデータを得て前記複数の記憶領域における何れかの記憶領域に格納する復号化手段

を備えることを特徴とする請求項 9 記載のシステム集積回路。

【請求項 11】 秘密データと、複数の命令からなるプログラムとを格納したメモリデバイスに接続されているシステム集積回路であって、

メモリデバイスに格納されたプログラムから命令を順次取り出して、解読する中央処理装置と、

複数の記憶領域を有する記憶手段とを備え、

前記プログラムには、

秘密データを読み込む旨の読出命令が、読み込まれた秘密データを利用した処理を行う旨の命令より前に配置されており、

前記システム集積回路は、

前記中央処理装置が読出命令を解読した際、メモリデバイスから秘密データを読み込んで、複数の記憶領域のうち、予め定められた記憶領域に格納する初期化手段

を備えることを特徴とするシステム集積回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、中央処理装置を初めとする様々な回路が集積されたシステム集積回路に関し、機器に組み込まれて、秘密データを扱う場合の改良に関する。

【0002】

【従来の技術】

半導体プロセス技術の急速な進歩に伴い、システム集積回路(システムLSI)を内蔵した機器が急速に普及しつつある。システムLSI内蔵型機器は、システムLSIと、1つ以上のメモリデバイスとを含み、セットトップボックス、携帯機器等幅広い分野において、利用されている。かかる機器を具現する回路要素のうち、ロ

ジック部分は、システムLSI内部に実装される。ロジック部分には、中央処理装置(CPU)や、これにより利用されるキャッシュメモリ、レジスタ、トランスポートストリームの多重分離を行うTSデコーダー、MPEGストリームのデコードを行うMPEGデコーダー等がある。これらをLSI内に集積させることにより、ロジック部分の安定動作が保証される。一方、プログラムやデータを格納するROMは、メモリデバイスとしてシステムLSI外部に実装される。データやプログラムがシステムLSI外部に実装されるため、システムLSIに対して改変を加えず、メモリデバイスの格納内容を書き換えることにより、データやプログラムを変更することができる。

#### 【 0 0 0 3 】

セットトップボックスのような機器では、有料放送の受信や有料コンテンツの再生等、ユーザに対する課金が必要になる場合があり、メモリデバイスは機器についての識別情報(機器ID)や、操作者についての識別情報(ユーザID)等秘密扱いが求められるデータ、いわゆる秘密データを格納せねばならない。しかしメモリデバイスの格納内容は、製品の内容を解析する技術、いわゆる”リバース解析”により暴露される危険性がある。そこで従来の機器にあっては、秘密データを暗号化した上でメモリデバイスに格納し、リバース解析が不法に行われることによる秘密データの露見を避けている。

#### 【 0 0 0 4 】

秘密データは暗号化された状態でメモリデバイスに格納されているので、機器に対するハッキング行為を好適に防御することができる。

#### 【 0 0 0 5 】

##### 【発明が解決しようとする課題】

ところでメモリデバイスの格納時において秘密データは万全に暗号化されているとはいえ、メモリデバイスに格納されているプログラムは、暗号化がなされていない場合が多い。CPUのニーモニック表を参照しながらプログラムを逆アセンブルしてゆけば、CPUがどのような処理をするかを伺いすることができる。上述したような機器IDやユーザIDは、CPUの初期動作時にメモリデバイスからシステムLSIに取り込まれることが多いので、CPUの初期動作時において、システムLSI

内のCPUからメモリデバイスに発行される読出コマンドを解析すれば、メモリデバイスに格納されている秘密データが、システムLSIに内蔵されている複数のレジスタ、メモリのうちどれに格納されるかを伺い知ることができる。

【0006】

秘密データは、復号化部により暗号化が解除された状態でシステムLSI内部のレジスタ、メモリに格納されるので、解読により知り得た読出先を手掛かりにして、より詳細なリバース解析を行えば、暗号化がなされていない状態の秘密データを知得することができる。そうして得た秘密データが、悪意の第三者の手に渡れば、機器に対するハッキング行為が横行する恐れがあり、機器を製造したメーカーや有料放送・有料コンテンツを扱う業者は多大な打撃を被ってしまう。

【0007】

プログラムを暗号化する等、プログラムの逆アセンブラさえ防止できれば、秘密データの露見は防げるように思える。しかしリバース解析の技術進歩は目覚ましく、CPUが動作を行う際の僅かな痕跡がシステムLSI外部から観測されれば、これを手掛かりとして秘密データの読出先が突き止められることも考えられる。今後、電子マネーの取り扱い等を上述した機器に求める場合には、かかるリバース解析の進歩に対して抜本的な対処をシステムLSIに施しておくことが、システムLSIを製造するメーカーの責務になると考えられる。

【0008】

本発明の目的は、システムLSI内部におけるCPUの動きがトレースされようとも、メモリデバイスに格納された秘密データの読出先の露見を防ぐシステム集積回路を提供する。

【0009】

【課題を解決するための手段】

上記目的を達成するため、本発明に係るシステム集積回路は、中央処理装置と、複数の記憶領域を有する記憶手段と、機器に対する起動操作が操作者によりなされれば、メモリデバイスから秘密データを読み出して、記憶手段における複数領域のうち予め定められた記憶領域に当該秘密データをセットし、その後中央処理装置に対して動作開始を指示する初期化手段とを備えることを特徴としている



## 【 0 0 1 0 】

## 【発明の実施の形態】

以降図面を参照しながら、システム集積回路（システムLSI）の実施形態について説明する。

## （第 1 実施形態）

本実施形態に係るシステムLSIは、セットトップボックス内に実装されている。図 1 は、システムLSIを実装したセットトップボックスの内部構成を示す図である。セットトップボックスとは、衛星放送、地上波、有線の何れかから伝送されてくる放送波を受信して、これに含まれているトランスポートストリームの多重分離を行い、更にこれを復号して映像信号、音声信号等を出力する機器であり、テレビジョン受像機やパーソナルコンピュータ等と組み合わせて一般家庭内で用いられる。

## 【 0 0 1 1 】

図 1 に示すように、セットトップボックスは、メモリデバイス 1 0 1、1 1 1、フロントエンド部 1 0 2、周辺デバイス 1 0 3、外部リセット信号発生器 1 0 4、クロック信号発振器 1 0 5 を備える。

メモリデバイス 1 0 1、1 1 1 は、機器の動作を実現するプログラムや、データ、機器ID、ユーザIDを格納するためのEEPROM、SDRAMであり、バス、制御線を介してシステムLSIと接続されて二次記憶を構成する。これら各種データのうち、機器ID、ユーザIDは守秘が求められるデータであり、暗号化されてメモリデバイス 1 0 1、1 1 1 に格納される。守秘が求められるデータを暗号化する際のアルゴリズムは、いわゆる”ビットシャッフリング”と呼ばれるものである。このアルゴリズムは、元の機器ID、ユーザIDを構成するビットデータを所定の規則性をもって入れ替えるというものであり、暗号化された機器ID、ユーザIDを、同じ規則性をもって、入れ替えることで、元の機器ID、ユーザIDを得ることができる。

## 【 0 0 1 2 】

フロントエンド部 1 0 2 は、衛星放送アンテナ等が受信した放送波を復調して

、MPEG2規格に規定されたトランスポートストリームをシステムLSIに順次出力する。

周辺デバイス103は、フロントパネル、リモコン送受信部を備える。

外部リセット信号発生部104は、機器に対する起動操作がなされれば、外部リセット信号を出力する。

#### 【0013】

クロック信号発振器105は、機器に対する起動操作がなされれば、クロック信号を出力する。

セットトップボックスの機能を実現するロジック部分は、このシステムLSI内で実現されるので、セットトップボックス内の基板配線は、極めてシンプルに構成されている。

#### 【0014】

セットトップボックス内の基板配線がシンプルになった反面、システムLSI内部には、様々な構成要素が高密度に実装されることとなる。図2を参照しながらシステムLSIの内部構成に、どのような構成要素が実装されているかを説明する。図2に示すように、システムLSIは、トランスポートデコーダ1、AVデコーダ2、周辺デバイスインターフェイス3、SRAM4、レジスタファイル5、クロスバススイッチ6、CPU7、命令キャッシュ8、データキャッシュ9、フェッチ部10、命令デコーダ11、算術演算回路12、バスアクセス制御部13、暗号変換装置14、及び初期状態管理装置15からなる。

#### 【0015】

トランスポートデコーダ1は、フロントエンド部102から出力されるトランスポートストリームに対して多重分離を行って、MPEG2規格に規定されたビデオストリーム、オーディオストリームを得て、AVデコーダ2に出力する。

AVデコーダ2は、多重分離されたビデオストリーム-オーディオストリームを復号して、映像信号、音声信号を得る。

#### 【0016】

周辺デバイスインターフェイス部3は、周辺デバイス103におけるフロントパネル、リモコン送受信部とのインターフェイスである。

SRAM4は、メモリデバイス101、111に格納されているデータの一部を格納する。

レジスタファイル5は、メモリデバイス101、111に格納されているデータの一部を格納する。メモリデバイス101、111を二次記憶と称呼したのに対し、これらSRAM4、レジスタファイル5を一次記憶と称する。

#### 【0017】

クロスバススイッチ6は、データバス、I/Oバス、アドレスバス、命令バスの相互接続を行う。

中央処理装置(CPU)7は、命令についてのキャッシュメモリ(命令キャッシュ8)及びデータについてのキャッシュメモリ(データキャッシュ9)を介してクロスバススイッチ6と接続され、システムLSI内の統合制御を行う。CPU7は、命令キャッシュ8及びデータキャッシュ9を介してメモリデバイス101、111から命令を取り出すフェッチ部10と、取り出された命令を解読する命令デコーダ11と、解読結果に従って、メモリデバイス101、111からシステム集積回路に読み出されたデータを用いた演算を行う算術演算回路(ALU)12とを備えている。このことは図2においてCPU7に対応する枠内に示す通りである。

#### 【0018】

バスアクセス制御部13は、CPU7からの指示に従ってメモリデバイス101、111に対する読み書きを行う。以降バスアクセス制御部13の処理の詳細を、文節(13.i)、(13.ii)、(13.iii)、(13.iv)に分けて説明する。

(13.i)メモリデバイス101、111からの読み出し時にあたってバスアクセス制御部13は、二次記憶における格納内容をデータバスに出力するよう、制御線を通じて二次記憶に指示する。データバスに対して格納内容が順次出力されれば、バスアクセス制御部13はこれら格納内容を順次取り込んでゆき、一次記憶に格納する。

#### 【0019】

(13.ii)メモリデバイス101、111への書き込み時にあたってバスアクセス制御部13は、一次記憶の格納内容をデータバスに順次出力してゆく。それと共に、この格納内容の取り込みを行うよう、制御線を通じてメモリデバイス10

1、111に指示する。かかる指示に従ってメモリデバイス101、111がデータバスの伝送内容の取り込みを行えば、システムLSIからメモリデバイス101、111へのデータ書き込みがなされる。

【0020】

(13.iii)バスアクセス制御部13によるメモリデバイス101、111に対する読み書きは、CPU7からの制御に従って行われるが、初期状態管理装置15からの制御に従って行われる場合もある。つまりCPU7がプログラムを構成するプログラムを読み込む際、又は、プログラムの実行に伴ってデータの読み書きを、メモリデバイス101、111に対して行う際、バスアクセス制御部13はCPU7の制御下で、メモリデバイス101、111のアクセスを行う。一方初期状態管理装置15の制御下で、メモリデバイス101、111のアクセスを行うのは、機器の起動時において、メモリデバイス101、111に格納されている秘密データを読み込むという場合である。

【0021】

(13.iv)制御線を通じたアクセス指示は、バスアクセス制御部13がセレクト信号、アドレス信号、コマンド信号といった3種類の信号を出力することによりなされる。セレクト信号は複数のメモリデバイス101、111のうち、何れを選択するかを示す信号であり、アドレス信号は、セレクト信号により選択されたメモリデバイス101、111において、何れのアドレスをアクセスするかを示す信号である。コマンド信号は、このアクセスの内容が、読み出し／書き込みの何れであるかを示す。

【0022】

暗号変換装置14は、バスアクセス制御部13によりシステムLSI内部に取り込まれた格納内容が、秘密データであれば、これの暗号化を解除して原データを得た後、一次記憶を構成するキャッシュメモリ、レジスタの何れかに格納させる。一次記憶に秘密データが格納されており、これを書き込むようCPU7から指示されれば、これを暗号化した後にバスアクセス制御部13に出力し、メモリデバイス101、111に格納させる。

【0023】

初期状態管理装置 1 5 は、ユーザにより機器の起動が開始されると、所定の第 1 期間経過後、メモリデバイス 1 0 1、1 1 1 から機器 ID、ユーザ ID を読み出すようバスアクセス制御部 1 3 に対して指示を行い、所定の第 2 期間経過後、初期状態管理装置 1 5 に動作を開始させるべく、内部リセット信号を出力する。上述した第 1 期間、第 2 期間の経過を待つのは、セットトップボックス全体のハードウェアを安定させないと、CPU やメモリデバイスの正常動作が保証できないからである。第 1 期間、第 2 期間の経過を監視すべく、初期状態管理装置 1 5 はカウンタを有している。

#### 【 0 0 2 4 】

ここで機器の起動とは、機器に供給される電源電圧が所定の電圧値になり、外部リセット信号が LOW から HIGH に立ち上がることをいう。機器に対する電源投入時からしばらくした後、クロック発振器 1 0 5 によるクロック信号の発生が開始される。

初期状態管理装置 1 5 の処理の時間的推移を示したのが図 3 に示すタイミングチャートである。本図の第 1 段目は、機器外部における電源レベルを示し、第 2 段目は、外部リセット信号、第 3 段目はクロックパルス列からなるクロック信号、第 4 段目、第 5 段目は、クロックパルスの波数が 500 回、1000 回に達したときに初期状態管理装置 1 5 に内蔵されているカウンタにより出力される通知信号、第 6 段目は、初期状態管理装置 1 5 に対して発せられる内部リセット信号、第 7 段目は、バスアクセス制御部 1 3 により発せられる読出信号を示す。

#### 【 0 0 2 5 】

機器の起動操作がなされると、矢印 y1 に示すように電源が 0V から 5V に立ち上がる。その後、不定期間 y2 を経た後、クロック発振器 1 0 5 は、クロックパルスの出力を開始する。一方、外部リセット信号発生器 1 0 4 は、矢印 c1 に示すように外部リセット信号を LOW から HIGH に立ち上げる。クロックパルスの出力が開始され、外部リセット信号が LOW から HIGH に立ち上がれば、初期状態管理装置 1 5 に内蔵されているカウンタは、クロックパルスのカウントを開始する。カウント開始後、矢印 y3 に示すようにクロックパルスの波数が 500 個に達すれば、初期状態管理装置 1 5 内のカウンタは、バスアクセス制御部 1 3 内に通知信号 p1 を出力す

る。通知信号p1が出力されれば、バスアクセス制御部13は機器ID、ユーザIDを読み出すようメモリデバイス101、111に対して、読出信号p3を出力する。

## 【0026】

その後、矢印y4に示すように第2期間が経過し、クロックパルスの波数が1000個に達すれば、初期状態管理装置15内のカウンタは通知信号p2を出力する。バスアクセス制御部13に内部リセット信号c2をLOWからHIGHに立ち上げる。内部リセット信号c2が立ち上がれば、CPU7はメモリデバイス101、111からプログラムを構成する命令を読み出して実行するようバスアクセス制御部13を制御する。

## 【0027】

以上のように本実施形態に係るシステムLSIによれば、セットトップボックスの起動にあたって、メモリデバイス101、111に格納された秘密データをシステムLSI内部に読み込んだ後に、CPU7に動作開始を指示するので、たとえ悪意の第三者がシステムLSI外部からCPU7の動作をトレースしようとしても、秘密データが読み込まれた読出先の所在を悪意の第三者は特定することができない。システムLSI内部における読出先の所在という手掛かりを与えないので、秘密データの読出先を特定しようという悪意の行為の出鼻をくじくことができる。これにより、セットトップボックスに対するハッキング行為を未然に防止することができる。

## 【0028】

## (第2実施形態)

第1実施形態では、秘密データがバス上を伝送するので、ロジックアナライザ等の機器をバスと接続してバスの伝送内容を観測すれば、暗号化された状態の秘密データを知得することができる。暗号化されているとはいえ、露見された秘密データに対してより詳細なリバース解析を行うことにより、機器ID、ユーザIDが露見されてしまう恐れがある。本実施形態では、バスの伝送内容が観測された場合であっても、秘密データの露見を防ぐような改良を提案する。

## 【0029】

第2実施形態における機器の内部構成を図4に示す。本図に示すように、第2

実施形態では、バスアクセス制御部 1 3 とメモリデバイス 1 0 1、1 1 1 とを専用のシリアル線 2 1 で接続している。

第 1 実施形態では、秘密データを命令、他のデータと同様に扱い、データバス上で伝送させていたが、第 2 実施形態においてシステム LSI は、秘密データをバス上で伝送させず、この専用のシリアル線 2 1 上で伝送させる。メモリデバイス 1 0 1、1 1 1 からシステム LSI への秘密データの伝送をシリアル線 2 1 上で行えば、たとえバスの伝送内容がロジックアナライザ等でリバース解析されたとしても、秘密データが露見することはない。シリアル線 2 1 を通じて秘密データを伝送するという点で、守秘性は担保されているので、この実施形態においては、暗号変換装置 1 4 をシステム LSI に設けず、暗号化しない状態で、秘密データをメモリデバイス 1 0 1、1 1 1 に格納してもよい。

#### 【 0 0 3 0 】

##### （第 3 実施形態）

第 1 実施形態では、二次記憶をメモリデバイス 1 0 1、1 1 1 にて構成したが、本実施形態では 1 つのメモリデバイス 1 0 1 にて二次記憶を構成することを提案する。第 3 実施形態における機器の内部構成を図 5 に示す。

図 5 においてシステム LSI は、バス制御を行うバスアクセス制御部 1 3 に代えて、単一のメモリデバイス 1 0 1、1 1 1 に対する制御を行うデバイスアクセス制御部 3 1 を備えている。システム LSI によるメモリデバイス 1 0 1、1 1 1 の制御が制御線を介して行われる点は、第 1 実施形態と同様である。第 1 実施形態においてバスアクセス制御部 1 3 は、データ伝送をバス上で行っていたが、第 3 実施形態におけるデバイスアクセス制御部 3 1 は、データ伝送を、シリアル線 3 2 上で行っている。

#### 【 0 0 3 1 】

システム LSI は単一のメモリデバイス 1 0 1、1 1 1 に対してアクセス制御を行えばよいので、バスを介して制御を行う場合と比較して、システム LSI による構成の簡易化を具現することができる。またバスに対するリバース解析と比較して、シリアル線に対するリバース解析は困難なので、秘密データを暗号化せずとも、秘密データの露見を効率的に防御することができる。

## 【0032】

## (第4実施形態)

第1実施形態では、機器の起動時にメモリデバイス101、111に格納されている秘密データを、システムLSI内部に取り込んだが、第4実施形態ではかかる起動時ではなく、CPU7が秘密データを必要とした場合、メモリデバイス101、111からシステムLSI内に秘密データを読み込むことを提案する。かかる秘密データの読み込みを実現するため、第1実施形態に示した①メモリデバイス101、111、②CPU7、③初期状態管理装置15に対して改良を加えている。以下、第4実施形態に係る改良点について説明してゆく。

## 【0033】

①第4実施形態におけるメモリデバイス101、111が、第1実施形態に示したそれと第1に異なるのは、メモリデバイス101、111により格納されるプログラム内に、秘密データを複数の記憶領域のうち何れかに読み込む旨の読出命令が存在する点である。第2に異なるのは、このプログラムにおいて、この秘密データについての読出命令が、読み込まれた秘密データを利用する命令より前に配置されている点である。この秘密データについての読出命令が、他の読出命令と異なるのは、秘密データの読出先が明示されていない点である。そのため、たとえメモリデバイス101、111におけるプログラムを逆アセンブルした者が、この秘密データについての読出命令の存在に気付いたとしても、秘密データが果たしてどの記憶領域に格納されるかを特定することはできない。

## 【0034】

②第4実施形態におけるCPU7が、第1実施形態に示したそれと異なるのは、秘密データについての読出命令をメモリデバイス101、111から読み込んでこれを解読した際、読取要求を初期状態管理装置15に発行する点である。

③第4実施形態における初期状態管理装置15は、機器の起動時に秘密データを読み込もうとはせず、読取要求がCPU7から発行された際、メモリデバイス101、111から秘密データを読み出して、一次記憶のうち、予め定められた記憶領域に設定する。秘密データが一次記憶に格納されれば、この秘密データを用いた処理をCPU7が行う。



## 【0035】

以上のように初期状態管理装置15が、CPU7が読出命令を解読して、秘密データの読取要求を発行した際、秘密データを読み込むので、秘密データの読み込み時期は、機器の起動時に限定されない。そのため悪意の第三者が機器の起動時におけるデータのやりとりを詳細にリバース解析して、秘密データの取得を企てようとも、彼等の執拗なリバース解析をかわすことができる。

## 【0036】

尚、本実施形態においてメモリデバイス101、111とシステムLSIとをシリアル線で接続し、秘密データの伝送をシリアル線を介して行っても良い。

## (第5実施形態)

第1実施形態において機器の機能を具現するデータ、プログラムはメモリデバイス101、111に格納されていることが明らかである。よってこのメモリデバイス101、111の格納内容がそっくりそのまま他の記録媒体にコピーされれば、機器で使用されているプログラム、データの複製物が容易に作成されてしまう。第1実施形態では、機器ID、ユーザIDのみを暗号化して、メモリデバイス101、111に格納していたが、第5実施形態では、メモリデバイスに格納されるべき全てのデータを、このメモリデバイス101、111に固有な暗号鍵（デバイス鍵）を用いて暗号化して格納することにより、デッドコピーの防止を実現している。

## 【0037】

図6は、第5実施形態に係るシステムLSIの内部構成を示す図である。図6が図2と異なるのは、図6には暗号変換装置14は存在せず、システムLSI内部のクロスバススイッチ6と、バスアクセス制御部13との間に暗号変換装置50が設けられている。

また第1実施形態において初期状態管理装置15は、起動時から第1期間経過後に機器ID、ユーザIDをメモリデバイス101、111から読み出すようバスアクセス制御部13を制御したが、第5実施形態において初期状態管理装置15は、同じ第1期間経過後に、暗号化された状態のデバイス鍵を読み出すよう、バスアクセス制御部13を制御する。

## 【0038】

暗号変換装置50の内部構成を図7に示す。図7に示すように暗号変換装置50は、デバイス鍵復号部51、デバイス鍵格納部52、EX-OR演算部53、EX-OR演算部54、EX-OR演算部55を備える。

デバイス鍵復号部51は、メモリデバイスから暗号化されたデバイス鍵が読み出されれば、このデバイス鍵を復号して、元のデバイス鍵を得る。

## 【0039】

デバイス鍵格納部52は、デバイス鍵復号部51により暗号化が解除されたデバイス鍵を格納する。

EX-OR演算部53は、メモリデバイス101、111に書き込むべきデータと、デバイス鍵とのEX-OR演算を行い、その結果をバスアクセス制御部13に出力する。これによりメモリデバイス101、111に書き込むべきデータは、メモリデバイス101、111に固有のデバイス鍵にて、暗号化されることになる。

## 【0040】

EX-OR演算部54、55は、メモリデバイス101、111から読み出されたデータ又は命令と、デバイス鍵とのEX-OR演算を行い、その結果を一次記憶に出力する。これによりメモリデバイス101、111内において、データ又は命令がメモリデバイス101、111に固有なデバイス鍵にて暗号化されていたとしても、メモリデバイス101、111からのデータ読み出し時において、この暗号化は解除されることになる。

## 【0041】

メモリデバイス101、111に対するデータ読み書きにあたって、EX-OR演算部53～55がデバイス鍵と、データとのEX-OR演算を行うのでデータを、メモリデバイス101、111固有のデバイス鍵により暗号化した状態で、メモリデバイス101、111に格納しておくことができる。

以上のように本実施形態によれば、メモリデバイス101、111に格納させるべきデータを、メモリデバイス101、111に固有なデバイス鍵を用いて暗号化した後、メモリデバイス101、111に格納するので、たとえ悪意の第三者がメモリデバイス101、111の格納内容をデッドコピーしたとしても、プ

プログラム、データを他の機器で利用することができない。これによりプログラム、データの守秘性や著作権は好適に保護される。

【 0 0 4 2 】

また暗号化に用いられるデバイス鍵は、CPU 7 の動作開始に先だって、システムLSI内に取り込まれるので、悪意の第三者がCPU 7 の動作をトレースしたとしても、デバイス鍵が露見する確率は低い。

尚、本実施形態においてメモリデバイス 1 0 1、1 1 1 とシステムLSIとをシリアル線で接続し、秘密データの伝送をシリアル線を介して行っても良い。

【 0 0 4 3 】

【発明の効果】 以上のように本発明に係るシステム集積回路は、中央処理装置と、複数の記憶領域を有する記憶手段と、機器に対する起動操作が操作者によりなされれば、メモリデバイスから秘密データを読み出して、記憶手段における複数領域のうち予め定められた記憶領域に当該秘密データをセットし、その後中央処理装置に対して動作開始を指示する初期化手段とを備えている。機器の起動にあたって、メモリデバイスに格納された秘密データをシステム集積回路内部に読み込んだ後に、中央処理装置に動作開始を指示するので、たとえ悪意の第三者がシステム集積回路外部から中央処理装置の動作をトレースしようとしても、秘密データが読み込まれた読出先の所在を悪意の第三者は特定することができない。システム集積回路内部における読出先の所在という手掛かりを与えないので、システム集積回路内部における秘密データの読出先を特定しようという悪意の第三者の行為の出鼻をくじくことができる。これにより、機器に対するハッキング行為を未然に防止することができる。

【 0 0 4 4 】

ここで前記機器は、操作者により起動操作がなされた際、外部リセット信号を出力する外部リセット信号出力手段と、複数のクロックパルスからなるクロック信号を出力するクロック発振手段とを備え、前記初期化手段は、外部リセット信号が出力されれば、クロックパルスの波数を計数するカウンタと、波数の計数値が第 1 の所定値になれば、メモリデバイスから秘密データを読み出して記憶手段における複数領域のうち、予め定められた記憶領域にセットする読出部と、波数

の計数値が、第1の所定値より大きい第2の所定値になれば、中央処理装置に対して内部リセット信号を出力して動作開始を指示する出力部とを備えてもよい。

【0045】

このシステム集積回路によれば、中央処理装置に対して内部リセット信号を出力する前に、メモリデバイスから秘密データを読み出すので、悪意の第三者がロジックアナライザを用いて中央処理装置の動作を観測したとしても、システムLSIにおける秘密データの読出先が露見することはない。

ここで前記秘密データは、機器についての識別情報又は機器を操作する操作者についての識別情報を暗号化して得た暗号化データであり、システム集積回路は、読出部により読み出された暗号化データを復号して、元の識別情報を得る復号化部を備え、記憶手段における複数の記憶領域のうち、予め定められた記憶領域は、復号により得られた元の識別情報を格納しても良い。

【0046】

このシステム集積回路によれば、電子マネー等の取り扱い時に利用される秘密データが、暗号化されてメモリデバイスに格納されるので、たとえ悪意の第三者がメモリデバイスの格納内容をデッドコピーしたとしても、悪意の第三者は秘密データを取得することができない。

ここでシステム集積回路はメモリデバイスと共に、機器に組み込まれ、機器においてメモリデバイスは、バス及びシリアル線を介してシステム集積回路と、接続されており、前記初期化手段は、機器に対する起動操作が操作者によりなされれば、秘密データをシリアル線に出力するようメモリデバイスに指示し、その後、シリアル線に出力された秘密データを取り込み、命令又はデータを読み出す旨が中央処理装置により指示されれば、命令又はデータをバスに出力するようメモリデバイスを制御し、その後、バスに出力された命令又はデータを取り込み、データを書き込む旨が中央処理装置により指示されれば、データをバスに出力し、その後、バスに出力されたデータを取り込むようメモリデバイスを制御するアクセス制御部を備えてもよい。

【0047】

メモリデバイスからシステムLSIへの秘密データの伝送をシリアル線上で行え

ば、たとえバスの伝送内容がロジックアナライザ等でリバース解析されたとしても、秘密データが露見することはない。

ここで前記秘密データは、メモリデバイス固有のデバイス鍵であり、前記初期化手段は、機器に対する起動操作が操作者により指示されれば、メモリデバイスからデバイス鍵を読み出して、予め定められた記憶領域に格納し、前記システム集積回路は、中央処理装置によりデータ書き込みが命じられれば、書き込むべきデータを、記憶領域に格納されたデバイス鍵を用いて暗号化する暗号化手段と、暗号化されたデータをメモリデバイスに格納させるよう、メモリデバイスを制御するアクセス制御手段とを備えてもよい。このシステム集積回路によれば、メモリデバイスに格納させるべきデータを、メモリデバイスに固有なデバイス鍵を用いて暗号化した後、メモリデバイスに格納するので、たとえ悪意の第三者がメモリデバイスの格納内容をデッドコピーしたとしても、プログラム、データを他の機器で利用することができない。これによりプログラム、データの守秘性や著作権は好適に保護される。

【0048】

また暗号化に用いられるデバイス鍵は、中央処理装置の動作開始に先だって、システム集積回路内に取り込まれるので、悪意の第三者が中央処理装置の動作をトレースしたとしても、デバイス鍵が露見する確率は低い。

ここで秘密データと、複数の命令からなるプログラムとを格納したメモリデバイスに接続されているシステム集積回路であって、メモリデバイスに格納されたプログラムから命令を順次取り出して、解読する中央処理装置と、複数の記憶領域を有する記憶手段とを備え、前記プログラムには、秘密データを読み込む旨の読出命令が、読み込まれた秘密データを利用した処理を行う旨の命令より前に配置されており、前記システム集積回路は、前記中央処理装置が読出命令を解読した際、メモリデバイスから秘密データを読み込んで、複数の記憶領域のうち、予め定められた記憶領域に格納する初期化手段を備えていてもよい。中央処理装置が読出命令を発行した際、秘密データを読み込むので、秘密データの読み込み時期は、機器の起動時に限定されない。そのため悪意の第三者が機器の起動時におけるデータのやりとりを詳細にリバース解析して、秘密データの取得を企てよう

とも、彼等の執拗なりバース解析をかわすことができる。

【図面の簡単な説明】

【図 1】

システムLSIを実装したセットトップボックスの内部構成を示す図である。

【図 2】

システムLSIの内部構成を示す図である。

【図 3】

初期状態管理装置 1 5 の処理の時間的推移を示したタイミングチャートである。

【図 4】

第 2 実施形態におけるシステムLSIの内部構成を示す図である。

【図 5】

第 3 実施形態におけるシステムLSIの内部構成を示す図である。

【図 6】

第 5 実施形態におけるシステムLSIの内部構成を示す図である。

【図 7】

第 5 実施形態においてシステムLSIに設けられた暗号変換装置 5 0 の内部構成を示す図である。

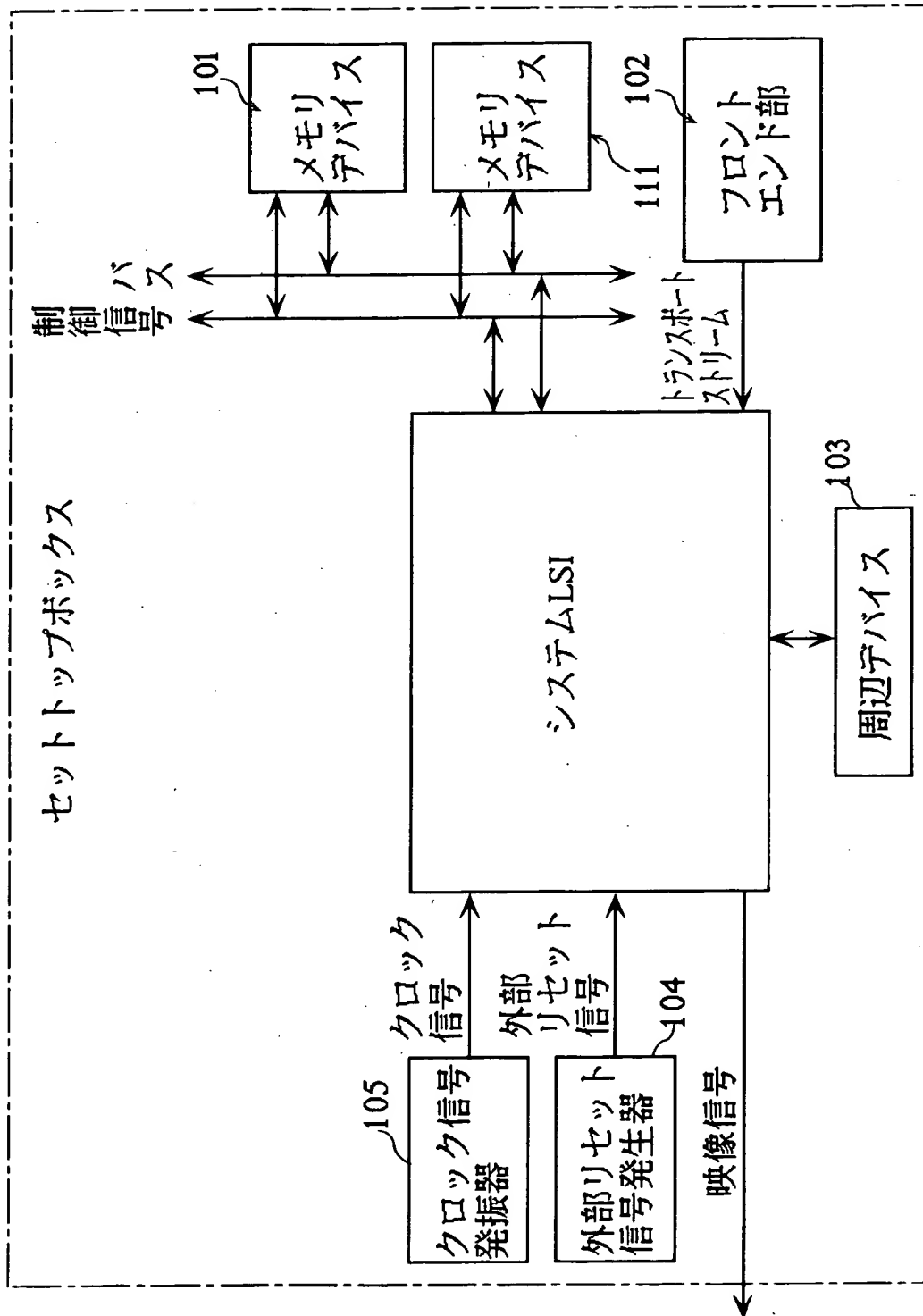
【符号の説明】

- 1     トランスポートデコーダ
- 2     AVデコーダ
- 3     周辺デバイスインターフェイス
- 4     SRAM
- 5     レジスタファイル
- 6     クロスバススイッチ
- 7     中央処理装置
- 8     命令キャッシュ
- 9     データキャッシュ
- 10    フェッチ部

- 1 1 命令デコーダ
- 1 2 算術演算回路
- 1 3 バスアクセス制御部
- 1 4 暗号変換装置
- 1 5 初期状態管理装置
- 2 1 シリアル線
- 3 1 デバイスアクセス制御部
- 3 2 シリアル線
- 5 0 暗号変換装置
- 5 1 デバイス鍵復号部
- 5 2 デバイス鍵格納部
- 5 3 ~ 5 5 EX-OR演算部
- 1 0 1、1 1 1 メモリデバイス
  - 1 0 2 フロントエンド部
  - 1 0 3 周辺デバイス
  - 1 0 4 外部リセット信号発生器
  - 1 0 5 クロック信号発振器

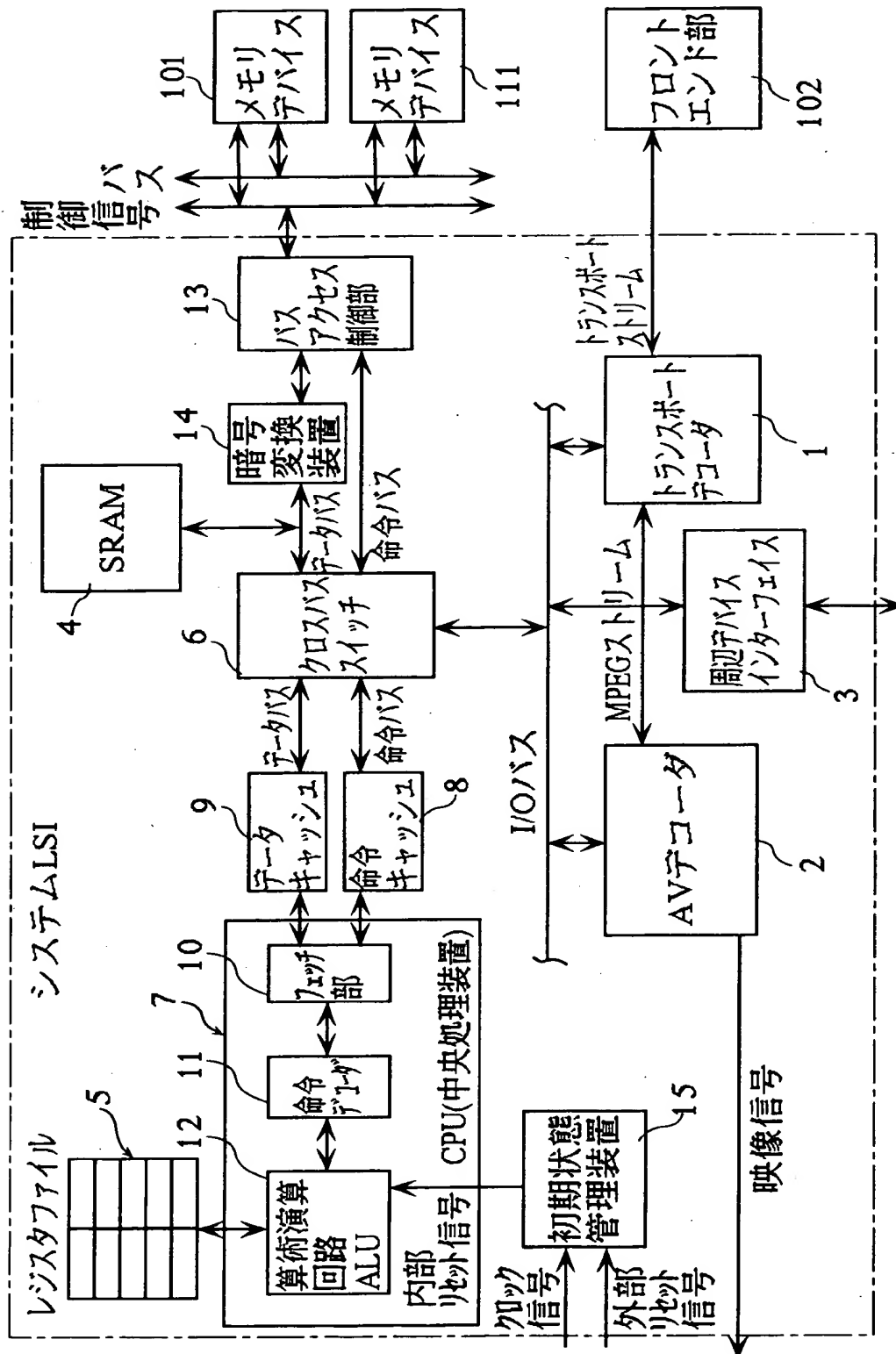
【書類名】 図面

【図 1】

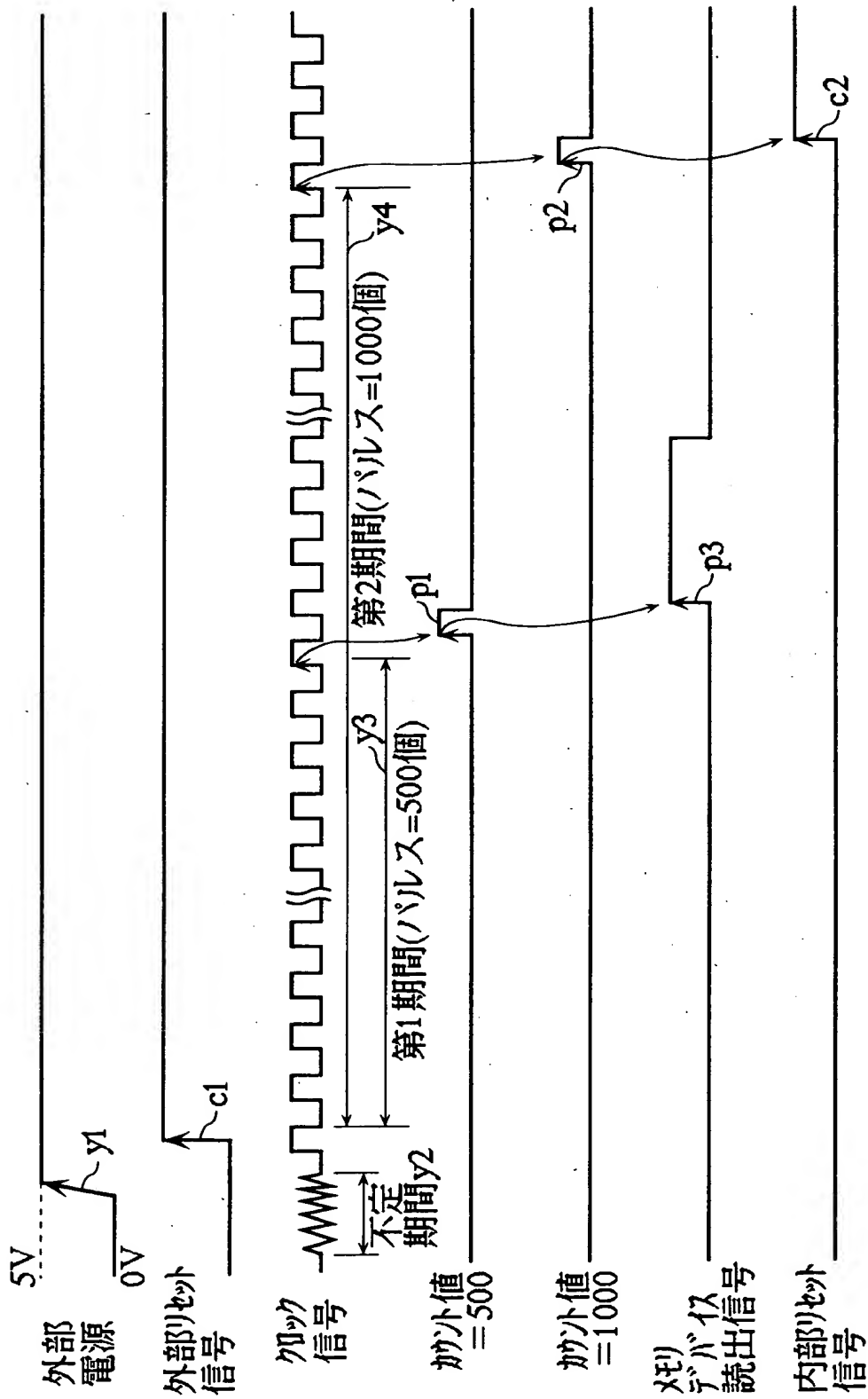




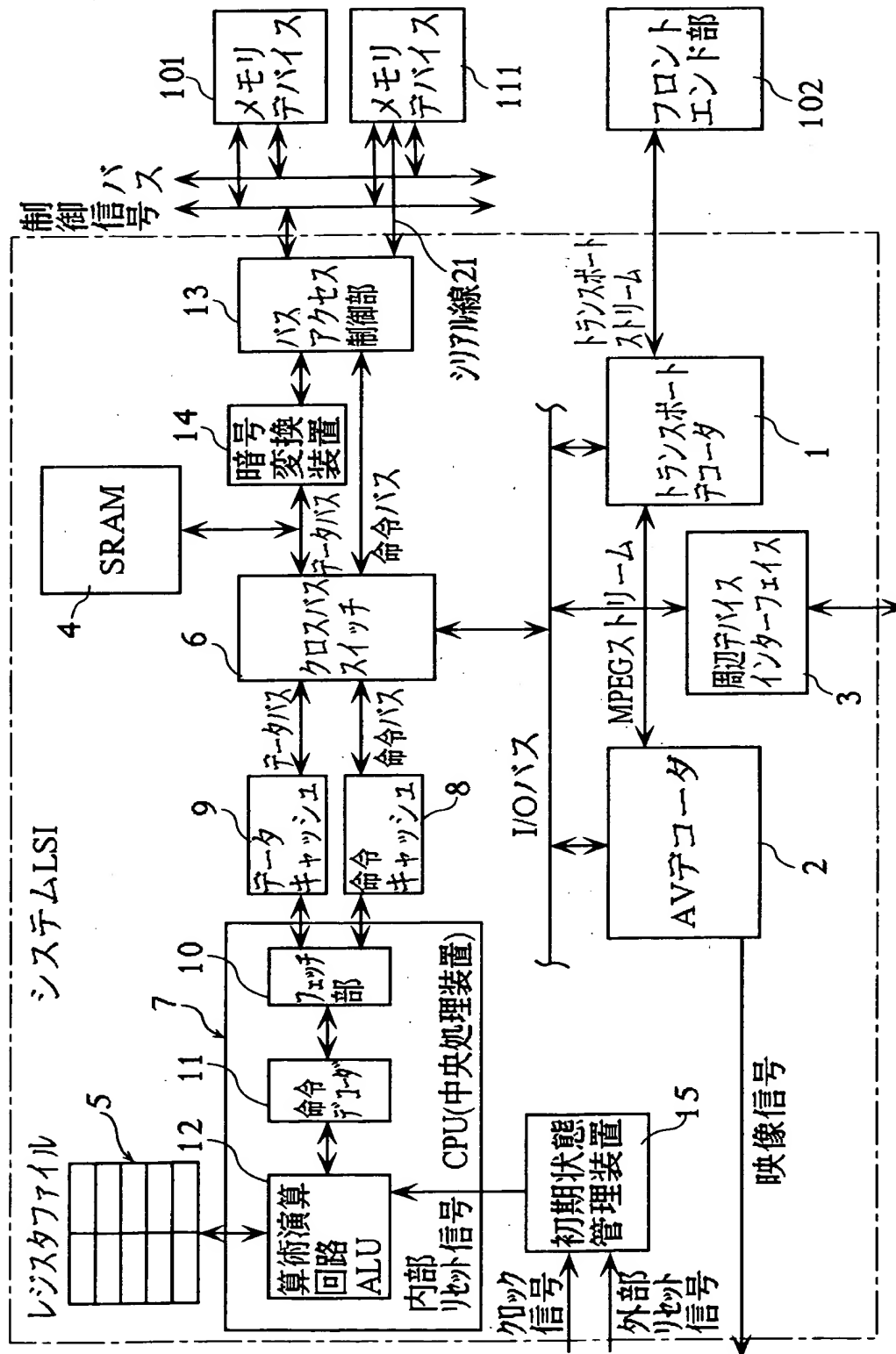
【図2】



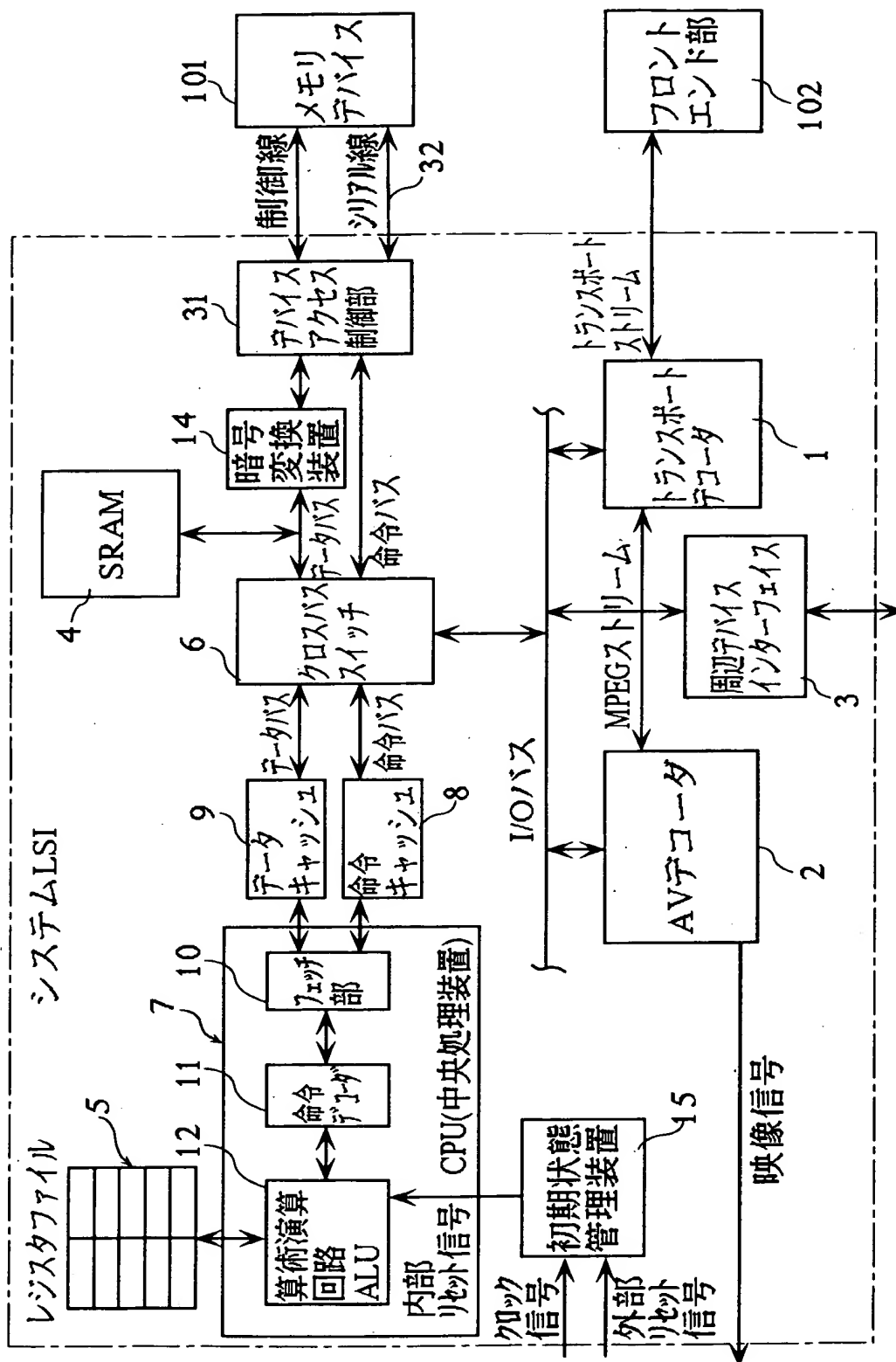
【図3】



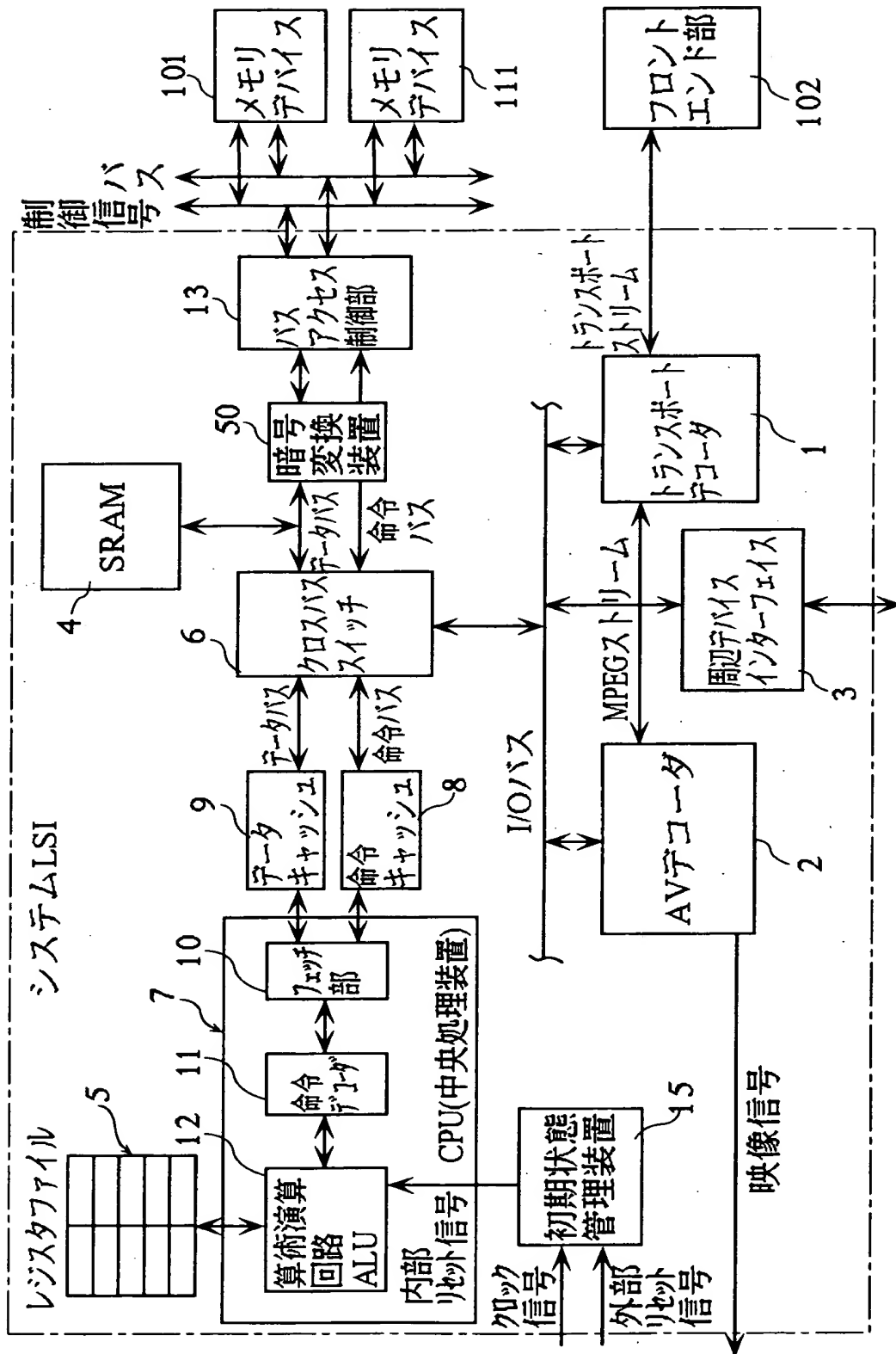
【図4】



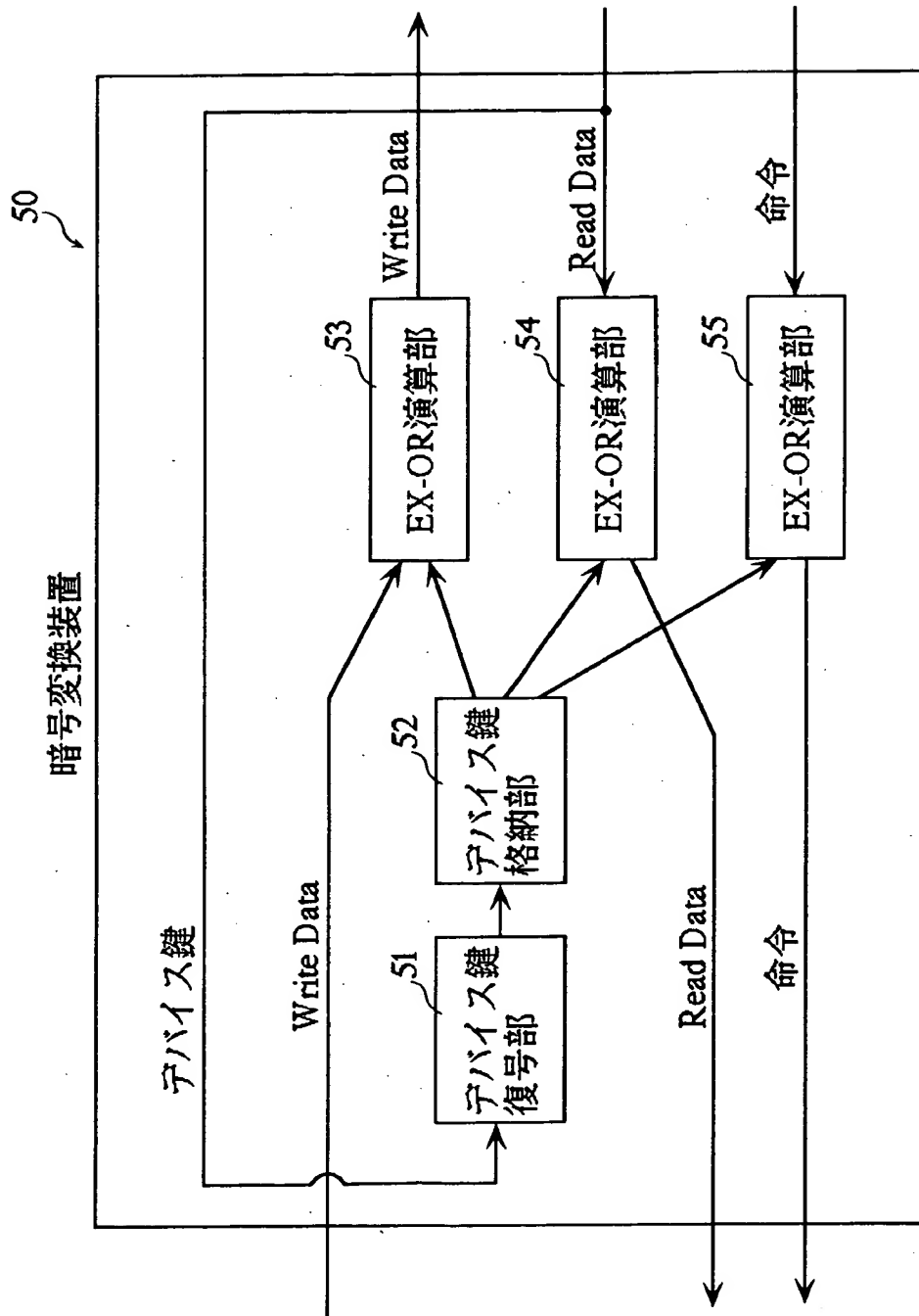
【図5】



【図6】



【図 7】



【書類名】 要約書

【課題】 内蔵されているCPUの動きがトレースされようとも、メモリデバイスに格納された秘密データの読出先の露見を防ぐシステム集積回路を提供する。

【解決手段】 二次記憶は、秘密データを格納しており、この秘密データは、CPU 7 により利用されるものである。二次記憶から一次記憶への読み出しはシステム集積回路が組み込まれている機器の起動時に行われる。即ち初期状態管理装置 1 5 は、機器に対する起動操作が操作者によりなされれば、メモリデバイス 1 0 1、1 1 1 から秘密データを読み出して一次記憶における複数領域のうち、何れかにセットする。その後、CPU 7 に対して動作開始を指示する。たとえCPU 7 の動作が詳細にリバース解析されようようとも、秘密データの読出先の露見を防ぐことができる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日  
[変更理由] 新規登録  
住 所 大阪府門真市大字門真1006番地  
氏 名 松下電器産業株式会社